PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY REPORT ON PATENTABILITY
(Chapter II of the Patent Cooperation Treaty)

(PCT Article 36 and Rule 70)

Applicant's or agent's file reference	FOR FURTHER ACTION See Form PCT/IPEA/416	
PE18901PC00		
International application No.	International filing date *(day/month/year)*	Priority date *(day/month/year)*
PCT/SE2004/001466	13-10-2004	14-10-2003
International Patent Classification (IPC) or national classification and IPC		
H04L9/08		
Applicant		
SELANDER, Göran et al		

1. This report is the international preliminary examination report, established by this International Preliminary Examining Authority under Article 35 and transmitted to the applicant according to Article 36.
2. This REPORT consists of a total of 3 sheets, including this cover sheet.
3. This report is also accompanied by ANNEXES, comprising:
   a. ☐ *(sent to the applicant and to the International Bureau)* a total of _____ sheets, as follows:
      ☐ sheets of the description, claims and/or drawings which have been amended and are the basis of this report and/or sheets containing rectifications authorized by this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions).
      ☐ sheets which supersede earlier sheets, but which this Authority considers contain an amendment that goes beyond the disclosure in the international application as filed, as indicated in item 4 of Box No. I and the Supplemental Box.
   b. ☐ *(sent to the International Bureau only)* a total of (indicate type and number of electronic carrier(s))
      _____, containing a sequence listing and/or tables related thereto, in electronic form only, as indicated in the Supplemental Box Relating to Sequence Listing (see Section 802 of the Administrative Instructions).
4. This report contains indications relating to the following items:
   - ☒ Box No. I Basis of the report
   - ☐ Box No. II Priority
   - ☐ Box No. III Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
   - ☐ Box No. IV Lack of unity of invention
   - ☒ Box No. V Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
   - ☐ Box No. VI Certain documents cited
   - ☐ Box No. VII Certain defects in the international application
   - ☐ Box No. VIII Certain observations on the international application

Date of submission of the demand	Date of completion of this report
12-05-2005	27-09-2005
Name and mailing address of the IPEA/SE Patent- och registreringsverket Box 5055 S-102 42 STOCKHOLM Facsimile No. +46 8 667 72 88	Authorized officer Jan Silfverling/MN Telephone No. +46 8 782 25 00

INTERNATIONAL PRELIMINARY REPORT ON PATENTABILITY

International application No.
PCT/SE2004/001466

Box No. I Basis of the report

1. With regard to the **language**, this report is based on:

☐ the international application in the language in which it was filed

☐ a translation of the international application into _____ ,
which is the language of a translation furnished for the purposes of:

☐ international search (Rules 12.3(a) and 23.1(b))

☐ publication of the international application (Rule 12.4(a))

☐ international preliminary examination (Rules 55.2(a) and/or 55.3(a))

2. With regard to the **elements** of the international application, this report is based on *(replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to this report):*

☒ the international application as originally filed/furnished

☐ the description:

pages _____ as originally filed/furnished

pages* _____ received by this Authority on _____

pages* _____ received by this Authority on _____

☐ the claims:

pages _____ as originally filed/furnished

pages* _____ as amended (together with any statement) under Article 19

pages* _____ received by this Authority on _____

pages* _____ received by this Authority on _____

☐ the drawings:

pages _____ as originally filed/furnished

pages* _____ received by this Authority on _____

pages* _____ received by this Authority on _____

☐ a sequence listing and/or any related table(s) – see Supplemental Box Relating to Sequence Listing.

3. ☐ The amendments have resulted in the cancellation of:

☐ the description, pages _____

☐ the claims, Nos. _____

☐ the drawings, sheets/figs _____

☐ the sequence listing *(specify)*: _____

☐ any table(s) related to the sequence listing *(specify)*: _____

4. ☐ This report has been established as if (some of) the amendments annexed to this report and listed below had not been made, since they have been considered to go beyond the disclosure as filed, as indicated in the Supplemental Box (Rule 70.2(c)).

☐ the description, pages _____

☐ the claims, Nos. _____

☐ the drawings, sheets/figs _____

☐ the sequence listing *(specify)*: _____

☐ any table(s) related to the sequence listing *(specify)*: _____

* *If item 4 applies, some or all of those sheets may be marked "superseded."*

INTERNATIONAL PRELIMINARY REPORT ON PATENTABILITY

International application No.
PCT/SE2004/001466

Box No. V **Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement**

1. Statement

Novelty (N)	Claims	1-32	YES
	Claims		NO
Inventive step (IS)	Claims	1-32	YES
	Claims		NO
Industrial applicability (IA)	Claims	1-32	YES
	Claims		NO

2. Citations and explanations (Rule 70.7)

Reference is made to the following documents:

D1: MENEZES,VANSTONE,OORSCHOT: Handbook of Applied Cryptography" 1997, CRC PRESS LLC , USA
D2: US 20030188158 A1
D3: EP 1050789 A

Document D1, which is considered to represent the most relevant state of the art, discloses a cryptographic system using one-way functions for derivation such that comprise of a current key does not comprise earlier keys, from which the subject-matter of claims 1-32 differs in that earlier generations of keys efficiently can be derived from later ones, but not the other way around, by use of a one-way key derivation function.

D2-D3 are only showing the state of the art.

The subject-matter of claims 1-32 is therefore novel and is considered to have inventive step and industrial applicability.